

**AFFIDAVIT OF SPECIAL AGENT ERIN FULLER IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, ERIN FULLER, state:

INTRODUCTION AND AGENT BACKGROUND

1. As a law enforcement officer of the United States, I am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in the United States Code (“U.S.C.”). I am a Special Agent with the United States Department of Health and Human Services, Office of Inspector General (“HHS-OIG”). I worked at the Boston office of HHS-OIG from August 2005 to April 2009 and from May 2016 to the present. I hold a Bachelor of Arts in Psychology.

2. As a Special Agent with HHS-OIG, I am responsible for investigating allegations of health care fraud affecting public health care benefit programs such as Medicare and Medicaid. I have participated in a variety of such investigations, during the course of which I have interviewed witnesses, conducted physical surveillance, executed arrest and search warrants, and reviewed various forms of evidence including website and email data, Medicare and Medicaid claims data, medical records, invoices, and other business records.

3. Through my training, education, and experience, I am familiar with a variety of fraud schemes involving public health care benefit programs. I have participated in numerous investigations into health care fraud and the provision of kickbacks to health care providers to induce the purchase of pharmaceuticals, medical devices, or medical services, in violation of 18 U.S.C. § 1347 (Health Care Fraud) and 42 U.S.C. § 1320a-7b (the Anti-Kickback Statute).

4. I am currently investigating Gustavo KINRYS (“KINRYS”) and the Boston Center for Clinical Research LLC (“BCCR”), and other as-yet unknown or unidentified (collectively, the “TARGET SUBJECTS”) for a number of offenses, including healthcare fraud, in violation of

18 U.S.C. § 1347, wire fraud in violation of 18 U.S.C. § 1343; false statements relating to healthcare matters in violation of 18 U.S.C. § 1035, and violation of the Anti-Kickback statute, 42 U.S.C. § 1320a-7b(b) (collectively, the “TARGET OFFENSES”). The investigation is a joint criminal investigation that the United States Attorney’s Office for the District of Massachusetts, and HHS-OIG (collectively, “the Investigative Team”) are conducting.

5. KINRYS is a psychiatrist. He owns BCCR, which is located at 67 Union Street, Suite 401, Natick, Massachusetts. (KINRYS has also referenced his practice at that same location as Advanced TMS Associates and Psychservices Counseling Center.) Based on the investigation to date, I submit that there is probable cause to believe that KINRYS and BCCR are billing Medicare and private insurers for various types of medical services that were not, in fact, provided.

PURPOSE OF AFFIDAVIT

6. I submit this affidavit in support of an application for a warrant under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure to search and seize records and data from the following e-mail accounts identified as the “TARGET ACCOUNTS” throughout this affidavit.

- gkinrys@bostonclinresearch.org – belonging to Gustavo KINRYS
- zcarvalho@bostonclinresearch.org – belonging to ZC
- azawadzka@bostonclinresearch.org – belonging to AZ
- tms1@bostonclinresearch.org – belonging to the first NeuroStar TMS Therapy System purchased by Gustavo KINRYS and BCCR
- anaornelas@bostonclinresearch.org – belonging to AO

- mbonorino@bostonclinresearch.org – belonging to MB
- tms2@bostonclinresearch.org – belonging to the second NeuroStar TMS Therapy System purchased by Gustavo KINRYS and BCCR.

7. I have probable cause to believe that these accounts – and Google calendars associated with these accounts – contain evidence, fruits, and instrumentalities of the crimes identified above, as described in the Attachment B associated with each of the TARGET ACCOUNTS.

8. Based on the e-mail addresses' domain name and information obtained during the investigation as described below, I have probable cause to believe that the accounts and relevant data are maintained by Google, Inc. by ("Google"), which, government databases indicate, accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via website <https://support.google.com/legal-investigations/contact/LERS> as described in the Attachment A associated with each of the TARGET ACCOUNTS.

9. The facts in this affidavit come from personal observations, training, experience, review of records, and information obtained from witnesses and other law enforcement officers. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during this investigation.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

10. The investigative team has developed information indicating that KINRYS has billed Medicare and private insurers for hundreds of thousands of dollars' worth of medical treatments and psychotherapy that he did not, in fact, render to his patients. Information that patients of KINRYS and former employees of BCCR have provided, as well as documents from

a third party reflecting KINRYS's use of certain medical devices, show that KINRYS misrepresented the amount and the frequency of medical treatments he provided to numerous patients. In early 2018, when Medicare and certain private insurers began to question the claims for reimbursement submitted on behalf of KINRYS, KINRYS began directing BCCR employees to create false documentation to provide (false) back-up for his claims for reimbursement. In addition, former patients have provided information indicating that KINRYS was routinely waiving patient copayments, which can amount to a violation of the Anti-Kickback Statute if done for Medicare beneficiaries.

11. Since early 2018, HHS-OIG has been investigating KINRYS and BCCR for questionable billing practices. Data from the Centers for Medicare & Medicaid Services ("CMS") revealed that Medicare paid KINRYS a total of \$840,349 between January 1, 2017 and March 30, 2018. The average amount CMS paid KINRYS per beneficiary was more than 30 times higher than the average CMS paid a provider in KINRYS's peer group. Over 66% of the amount paid to KINRYS represented payments for a treatment called Transcranial Magnetic Stimulation ("TMS") that KINRYS and BCCR purportedly provided to patients.

TMS Therapy and the NeuroStar TMS Therapy System

12. TMS is a noninvasive method of brain stimulation used to treat adults who have a confirmed diagnosis of major depressive disorder. Neuronetics, Inc. sells a medical device used to provide TMS therapy to patients called the NeuroStar TMS Therapy System. According to the FDA 510K, or Premarket Notification, for the NeuroStar TMS Therapy System, it is a computerized, electromechanical medical device that produces and delivers non-invasive, magnetic stimulation using brief duration, rapidly alternating, or pulsed, magnetic fields to

induce electrical currents directed at spatially discrete regions of the cerebral cortex. In addition to selling the NeuroStar TMS Therapy System device, Neuronetics also sells bundles of treatment sessions to doctors. The NeuroStar TMS Therapy System is designed so that the number of TMS treatment sessions a user (like KINRYS) can provide to patients is limited to the number of TMS treatment sessions that user (e.g., KINRYS) has purchased from Neuronetics.

13. A photograph of the NeuroStar TMS Therapy System is below:



14. According to Neuronetics' website, the NeuroStar TMS Therapy System is an in-office treatment that has been cleared to be performed in as little as 19 minutes (but may take up to 39 minutes due to patient sensitivity or at the discretion of the treating psychiatrist) per session. The treatment is performed while the patient is awake, alert and is seated and reclined in the NeuroStar treatment chair. Neuronetics literature states that a course of TMS treatment consists of sessions administered for five days a week for up to six weeks.

15. During a patient's first treatment session, two essential steps are performed. First,

the patient's cortex is mapped with the NeuroStar Treatment Coil to identify the motor cortex. Once the specific location on the motor cortex is found, the second step involves the use of a proprietary software algorithm, which assists the provider in estimating the physiologically appropriate magnetic field intensity for each treatment session. After these two steps are performed, the location of the motor cortex then also serves as a reference point to enable the psychiatrist to properly position the NeuroStar Treatment Coil over the prefrontal cortex, resting the coil lightly in contact with the patient's scalp. Once the coil is properly positioned, the device delivers NeuroStar TMS Therapy using a highly targeted, pulsed magnetic field to stimulate cortical neurons.

16. Medicare provides coverage for this TMS treatment and requires that a physician (MD or DO) who writes an order for the TMS treatment examine the patient and review the patient's record. Both CMS and private insurance carriers require that the physician have experience in administering TMS therapy and that the treatment be given under direct supervision of this physician. In other words, the physician must be in the area where the TMS therapy is being provided and be immediately available.

Waivers of Copayments and the Anti-Kickback Statute

17. Part of government's investigation into KINRYS and BCCR has focused on potential violations of the Anti-Kickback Statute ("AKS"). Under the AKS, it is illegal to provide "any remuneration" to induce a person to order goods under a federal health care program. *See* 42 U.S.C. 1320a-7b(b)(2). In passing the AKS, Congress intended the term "any remuneration" to be understood broadly. H. R. Rep. No. 95-393 (1977), at 53, in 1977 U.S.C.C.A.N.N. 3039, 3056 ("The bill would define the term 'any remuneration' broadly to

encompass kickbacks, bribes, or rebates which may be made directly or indirectly, overtly or covertly, in cash or in kind (but would exclude any amount paid by an employer to an employee for employment in the provision of covered items or services).”). Congress considered such inducements to “contribute significantly to the cost” of federal health care programs. *Id.* at 52, in 3055.

18. Since at least 1994, HHS-OIG has interpreted routine Medicare copayment waivers as violations of the AKS under certain circumstances. Publication of OIG Special Fraud Alerts, 59 Fed. Reg. No. 242 (page no. not available) (Dec. 19, 1994), available at <https://www.gpo.gov/fdsys/pkg/FR-1994-12-19/html/94-31157.htm>. The “[r]outine waiver of deductibles and copayments by charge-based providers, practitioners or suppliers is unlawful because it results in (1) false claims, (2) violations of the anti-kickback statute, and (3) excessive utilization of items and services paid for by Medicare.” The OIG’s rationale combined an understanding of the role of copayments in managing costs, on the one hand, with AKS inducement concerns, on the other: “At first glance, it may appear that routine waiver of copayments and deductibles helps Medicare beneficiaries. By waiving Medicare copayments and deductibles, the provider of services may claim that the beneficiary incurs no costs. In fact, this is not true. Studies have shown that if patients are required to pay even a small portion of their care, they will be better health care consumers, and select items or services because they are medically needed, rather than simply because they are free. Ultimately, if Medicare pays more for an item or service than it should, or if it pays for unnecessary items or services, there are less Medicare funds available to pay for truly needed services.” *Id.*

KINRYS's 2015 Purchase of the NeuroStar TMS Therapy System

19. In May 2015, KINRYS purchased a NeuroStar TMS Therapy System from Neuronetics for \$76,650. He also purchased 100 NeuroStar Treatment links or treatment sessions for \$9,800. KINRYS financed the purchase of the NeuroStar TMS Therapy System through Marlin Leasing Corporation. In doing so, he identified BCCR, located at 67 Union St, Suite 401, Natick, as the customer. The Neuronetics' customer enrollment form identifies KINRYS as the owner of BCCR and lists his physician's license number as 210468 and his email as kinrys@aol.com. The customer contact and billing contact listed on the Neuronetics-BCCR purchase documents is zcarvalho@bostonclinresearch.org.

20. KINRYS and BCCR began offering TMS therapy to patients at KINRYS's Natick-based psychiatry practice shortly after May 2015. KINRYS began billing Medicare for TMS therapy it supposedly provided to his patients beginning in June 2015. When doing so, KINRYS used the following current procedural terminology ("CPT") codes titled "therapeutic repetitive transcranial magnetic stimulation (TMS) treatment": 90867, 90868, and 90869.

21. Since June 2015, KINRYS has billed the following third party payors the following amounts for purportedly providing TMS therapy:

- BCBS: \$6.67 million (reimbursed \$1.8 million)
- Medicare: \$3.2 million (reimbursed \$815,000)
- Tufts Medical Plan: \$1.28 million (reimbursed \$319,000)
- Tufts Commercial: \$723,000 (reimbursed \$366,000)
- Optum: \$420,000

Medicare claims data indicates that KINRYS consistently has been among the top providers of

TMS therapy nationwide since he began billing for TMS in June 2015. He has billed for hundreds of TMS treatments to individual patients. Medicare claims data indicates that KINRYS typically provides TMS treatments to a patient at a frequency of five days per week for the patient's duration of TMS therapy (with the exception of major holidays).

22. Investigators have interviewed ZC and AZ, both of whom worked for KINRYS at BCCR. ZC worked for KINRYS at BCCR from 2013 until her resignation in July 2018.

According to documents obtained from Neuronetics, ZC was the administrator of KINRYS's and BCCR's NeuroStar account. Initially, ZC served as the sole TMS technician at BCCR. By the summer of 2015, KINRYS had hired another employee, AZ. Among other things, AZ assisted ZC with the TMS therapy. As the two TMS technicians for BCCR, ZC or AZ scheduled and assisted KINRYS with the initial TMS mapping session (billed under CPT code 90867) that he conducted on each new TMS patient. After a patient's initial session, ZC or AZ scheduled and administered the subsequent TMS sessions (billed under CPT code 90868) for all TMS patients. ZC typically worked at KINRYS's Natick office Monday through Thursday. AZ's hours increased over time and by the time she quit in April 2018, she was working Monday through Friday. KINRYS usually came to BCCR's office on Tuesdays and Wednesdays to see patients for psychotherapy and came into the office on some Thursdays primarily to conduct the initial TMS mapping sessions on new TMS patients.

KINRYS's False Billing for TMS Therapy Not Provided

Patient PM

23. Patient PM began seeing KINRYS in the late summer / early fall of 2016. According to Medicare systems data, KINRYS generally billed Medicare as though Patient PM

received TMS treatment 5 times per week. In total, KINRYS submitted claims to Medicare for 130 TMS treatments administered to Patient PM between November 28, 2016 and May 26, 2017 for a total amount billed of \$62,310. Medicare reimbursed KINRYS \$13,028 for the TMS services supposedly rendered to Patient PM.

24. According to Patient PM's wife, however, Patient PM did not receive TMS treatments in this amount or in this frequency. Specifically, Patient PM's wife noted that Patient PM never received TMS therapy at KINRYS's office 4-5 times per week. Instead, PM received TMS therapy – at most – three days per week, eventually tapering down to one day per week before stopping TMS therapy altogether. In September 2018, Patient PM's wife requested from BCCR a list of Patient PM's visits. The list of visits that BCCR emailed to Patient PM's wife (1) indicate that Patient PM received a total of 28 TMS treatments, which occurred between December 8, 2016 and April 4, 2017, and (2) corroborate Patient PM's wife's recollection in that it reflected that the frequency with which Patient PM typically received TMS treatments was 2-3 times per week – not 4-5 times per week.

25. Patient PM's wife's recollection is also corroborated by data from Neuronetics, the company that sold KINRYS and BCCR the two NeuroStar TMS Therapy systems KINRYS and BCCR used. Neuronetics maintains data showing when and how frequently BCCR and KINRYS used the two NeuroStar TMS Therapy systems Neuronetics sold to BCCR. Neuronetics' data shows that Patient PM received only 28 TMS treatments – far fewer than the 130 reflected in the Medicare systems data. The Neuronetics data also showed that Patient PM never received treatment 4-5 times per week.

26. On July 10, 2018, HHS-OIG issued a subpoena to KINRYS in which it requested

medical records for all services rendered to a number of KINRYS's patients, including Patient PM. In response to that subpoena, KINRYS produced a document called "Neurostar TMS Therapy Patient Report," which lists 115 TMS treatments administered to Patient PM by KINRYS or employees working for KINRYS – more than four times the number of TMS treatments Patient PM received according to internal BCCR records and internal Neuronetics data. KINRYS's signature appears at the end of the NeuroStar TMS Therapy Report produced to the government as part of KINRYS's subpoena response.

Patient RP

27. According to Medicare systems data, Patient RP began seeing KINRYS in August 2017. KINRYS billed Medicare \$70,200 for 147 separate TMS services KINRYS or BCCR purportedly provided to Patient RP between August 14, 2017 and March 9, 2018. Medicare data indicates Medicare reimbursed KINRYS \$14,763 for the TMS services supposedly rendered to Patient RP. According to ZC and AZ, Patient RP never received TMS therapy at KINRYS's office. At one point, Patient RP complained to AZ that her insurance had been improperly charged.

28. Contrary to what appears in the Medicare systems data, Neuronetics' records reveal that Patient RP received no TMS treatments at KINRYS's office. This documentation also corroborates the accounts provided by ZC and AZ.

Patient JR

29. Patient JR was referred to KINRYS in 2016 and began receiving TMS therapy at KINRYS's offices beginning in July 2016 and ending with her last TMS therapy session in the fall of 2017.

30. According to Medicare systems data, KINRYS billed Medicare \$184,760, for 387 separate TMS treatments purportedly provided to Patient JR between July 18, 2016 and February 9, 2018. That data reflects that Patient JR usually received the TMS treatments 5 times per week. Medicare data indicates KINRYS was reimbursed \$42,931 for the TMS services supposedly rendered to Patient JR.

31. Contrary to what appears in the Medicare systems data, Neuronetics records reveal that Patient JR received a total of 88 sessions of TMS therapy at KINRYS's office – far fewer than the 387 treatments reflected in the Medicare systems data.

32. Patient JR stated that she was never charged any amount, including any copayment, for services provided by KINRYS.

Patient IC

33. Patient IC is KINRYS's wife. According to Blue Cross Blue Shield of Massachusetts ("BCBSMA") claims data, KINRYS billed BCBSMA \$230,070 for TMS therapy supposedly provided to Patient IC. BCBSMA reimbursed KINRYS \$96,004 for TMS therapy supposedly provided to Patient IC.

34. According to ZC, Patient IC never received TMS therapy at KINRYS's office. AZ said she never saw Patient IC receiving TMS therapy at KINRYS's office. Consistent with ZC's and AZ's accounts, Neuronetics records reveal that Patient IC never received TMS treatments at KINRYS's office.

Patient SL

35. Patient SL became a patient of KINRYS's and BCCR in the fall of 2017 and began receiving TMS treatments at KINRYS's office in Natick at that time. Patient SL reported

that he received his last TMS therapy session at BCCR around the first week of January 2018.

36. According to Medicare systems data, KINRYS billed Medicare \$36,845 for 76 separate TMS services purportedly rendered to Patient SL between September 25, 2017 and January 12, 2018. Medicare reimbursed KINRYS \$8,462 for TMS therapy supposedly provided to Patient SL.

37. Patient SL reported that he maintains small red appointment books where he records various appointments, including visits to KINRYS's office. I have seen these red appointment books. Based on Patient SL's review of his 2017 and 2018 appointment books, Patient SL noted that – contrary to what was reflected in the Medicare systems data – he received TMS therapy at BCCR a total of 38 times on the following dates:

October 2017: 2, 4, 5, 10, 11, 12, 17, 18, 19, 24, 25, 27, and 30

November 2017: 1, 3, 6, 8, 10, 13, 15, 17, 20, 22, 27, and 29

December 2017: 1, 4, 6, 8, 11, 13, 15, 18, 20, 22, and 27

January 2018: 3 and 5.

38. Patient SL also reported that he received Explanation of Benefits (“EOB”) documents from his insurance providers. In reviewing those EOBs he received from his supplemental insurance provider, he noticed that someone had submitted claims for alleged TMS treatments provided to him on January 9-11, 2018. Patient SL had not, in fact, received TMS treatments during this time. Review of additional records shows that, during this three-day window, Patient SL actually was receiving inpatient care at MetroWest Medical Center for a gastrointestinal bleed, which would have prevented him from receiving TMS treatments at BCCR.

39. Consistent with Patient SL's report, Neuronetics records reveal that he received only 37 TMS treatments at KINRYS's office – far fewer than the 76 treatments KINRYS billed Medicare for.

40. As mentioned above, certain insurance carriers require that patients pay a copayment for the TMS treatments they receive. Patient SL reported that he never paid any money out-of-pocket for the TMS treatment he received. While there was a small amount of money that Patient SL's insurance did not cover and for which he was responsible, Patient SL reported that KINRYS told him that KINRYS "did fine" with the insurance reimbursement and did not need the patient's share. According to Patient SL, KINRYS said that because TMS was a frequent and intense therapy, he did not collect copayments from patients.

41. I have found additional examples where Medicare or private insurance companies were billed for TMS treatments KINRYS supposedly provided to patients, but where data from Neuronetics showed that those same patients either (a) received no TMS treatments at KINRYS's office, or (b) received far fewer TMS treatments at KINRYS's office than the number of treatments for which KINRYS was seeking reimbursement.

KINRYS and His Staff Store False Documentation Concerning KINRYS's Patients in a Dropbox.com Account

Dropbox Account

42. ZC, who worked for KINRYS at BCCR between 2013 and July 2018, reported that KINRYS and BCCR staff stored work-related documents in a Dropbox.com¹ account

¹ Dropbox is a file hosting service that offers "cloud" storage and file synchronization. Dropbox offers free and paid services that allow users to add photos, documents, videos and files to their account. Dropbox automatically saves these files to all of the user's computers, phones and to the Dropbox server, so they may be accessed from

installed on the computers at BCCR. AZ confirmed this. KINRYS set up the Dropbox account for the practice. Initially, KINRYS emailed a password for the practice's Dropbox account to ZC and another BCCR employee, AZ, so they could install the Dropbox on their desktop computers at KINRYS's office.

43. Once ZC had access to Dropbox on her computer at BCCR, she no longer needed to use the password to access and save documents to the Dropbox account. According to ZC, the files saved to the Dropbox account included prescriptions for KINRYS's patients, letters for KINRYS's patients, Neurostar TMS Therapy Patient Reports for KINRYS's patients, consent forms for KINRYS's patients, employee timesheets, and letters from insurance companies.

44. KINRYS worked from home at times. ZC said that KINRYS would save documents to Dropbox and alert ZC that the documents could be found in the Dropbox account. Sometimes, KINRYS would send ZC a link via email to a document in the Dropbox account so ZC could access the document at BCCR. ZC stated that KINRYS would sometimes send ZC and other BCCR employees an alert to access the Dropbox account.

KINRYS Directs AZ to Create False Reports of TMS Therapy

45. In February 2018, KINRYS began directing one of his staff members, AZ, to create false reports representing that certain patients of KINRYS's received TMS therapy when, in fact, they had not.

46. Around February 2018, KINRYS had received a number of medical records requests from insurers for specific patients. KINRYS asked AZ to (falsely) create a report for

anywhere. Dropbox offers a free plan that allows users to have 2 GB of space to store their files. Dropbox also offers plans that cost \$9.99 a month and allow users additional space on the Dropbox servers.

each of the patients identified in the medical record requests that would show that the patient received TMS therapy five days per week for a total of 36 sessions. AZ told KINRYS that the patients had not, in fact, received that many TMS sessions and that she did not feel comfortable creating the reports that represented that they had. Initially, KINRYS said OK and did not pressure her.

47. Later, however, KINRYS became upset that AZ had not created the false TMS reports for the patients he identified. KINRYS directed AZ to create a template that could be used to create the false TMS reports for the patients identified by KINRYS. AZ showed several templates to KINRYS, but KINRYS rejected them because they were “too detailed.” Ultimately, KINRYS approved a template AZ found and again told her to create records for patients showing that they had received TMS therapy five days per week for 36 sessions. I showed AZ a copy of a Neurostar TMS Therapy Patient Report that KINRYS produced in response to an HHS-OIG subpoena. AZ confirmed that the form of this Neurostar TMS Therapy Patient Report was the template AZ found and that KINRYS approved.

48. Initially, KINRYS gave AZ a list of approximately 20 patients for whom KINRYS ordered her to create reports showing – falsely – that those patients had received TMS therapy five days per week for 36 sessions. AZ noted that certain patients on that list had never received TMS therapy and told KINRYS it was wrong to create TMS reports for those patients. Despite this, KINRYS continued to pressure AZ to create TMS reports falsely reflecting that patients had received TMS therapy 5 days per week when, in fact, they had not.

49. KINRYS also provided AZ with direction regarding the content of the notes of the TMS reports. For example, KINRYS told AZ that the notes for each patient should change

over time to indicate that the patient was doing better. KINRYS told AZ that the notes could not look exactly the same. AZ saved the false TMS reports she created at KINRYS's direction in the Dropbox account KINRYS created for the office.

50. Later in the Spring of 2018, KINRYS increased his demands and ordered AZ to create TMS reports in response to all medical record requests that came into KINRYS's office from insurance companies. At one point, AZ told KINRYS that she was not going to make the TMS reports anymore. KINRYS responded that AZ had to do it, and that it was part of AZ's job. On or about April 4, 2018, KINRYS had the following exchange with AZ over text message:

KINRYS to AZ:

I don't think I can handle too many people tomorrow. Still sick.
But will try. Thank you for your help!
Do you think you can get to those TMS notes this week? Maybe Camila can help? we [*sic*] need to send some of those out.
Keep them simple. They look perfect.

AZ to KINRYS

Can we discuss this in the office tomorrow?

KINRYS to AZ

OK. But it has to be done. I don't have the time. It is part of the job.
That will not change.
That is not open for discussion.
Assign it to someone else. But it has to be done by someone.
I need them by the end of the week please.
Please stop overthinking things that you think you fully understand.

51. I have seen a screenshot of this text exchange between KINRYS and AZ on AZ's phone. On or about that same day, before AZ notified KINRYS of her decision to quit, she sent a text message to ZC's phone stating:

I am very sorry to do this to you [ZC], but this has really gotten too far. I can't be bullied by G to forge records. He was really mean to me and I don't want to be in this situation. I don't think I will come on Friday.

52. I have seen this text message from AZ on ZC's phone. According to ZC, ZC and AZ called KINRYS by his first name, Gustavo. ZC said that she understood "G" in the text message to refer to KINRYS.

53. ZC provided information consistent with what AZ reported. ZC stated that, at some point in February 2018, she learned that KINRYS had instructed AZ to create false records representing that certain patients of KINRYS received TMS therapy even in instances when those patients had not, in fact, received such therapy. At that time, ZC saw AZ with files that contained printed letters from insurance companies. Among other things, those letters requested that KINRYS turn over medical records for particular patients and particular dates of service.

54. ZC reported that AZ told ZC that KINRYS ordered AZ to create false notes relating to TMS therapy. At one point, AZ showed ZC what appeared to be a Microsoft Word document with the title "Neurostar TMS Therapy Patient Report" at the top of it. The report was up on AZ's desktop computer screen at the time, which was located in the reception area of BCCR. ZC stated that this was the first time she saw this type of document pertaining to TMS therapy, despite the fact that ZC had been working at BCCR since KINRYS had purchased the first NeuroStar TMS Therapy system from Neuronetics in 2015.

55. ZC reported that AZ told ZC that KINRYS was making AZ create NeuroStar TMS Reports for 36 days of TMS therapy for patients who did not, in fact, receive 36 sessions of TMS. ZC stated that KINRYS forced AZ to create the Neurostar TMS Reports, that AZ did not like creating the NeuroStar TMS Reports, and that AZ did not want to sign AZ's name to the

NeuroStar TMS Reports that AZ created.

56. AZ told ZC that AZ saved the false NeuroStar TMS Reports AZ created to the Dropbox file KINRYS had created. ZC has seen NeuroStar TMS Reports that AZ created in the Dropbox file. At KINRYS's instruction, ZC faxed some of the NeuroStar TMS Reports that AZ created to insurance companies in response to their medical records requests.

KINRYS Directs ZC to Create False TMS Reports

57. ZC stated that in May 2018, KINRYS approached her with a bag of letters from insurers – including letters seeking medical records – and told her, “These are what [AZ] started and I need you to continue.” KINRYS told ZC that ZC needed to finish the NeuroStar TMS Therapy Patient reports for every patient. KINRYS told ZC that he had told AZ to finish the NeuroStar TMS Reports for the Medicare patients; ZC believed that KINRYS thought AZ had completed those reports by the time AZ quit.

58. KINRYS instructed ZC to create a NeuroStar TMS Report for each patient with notes for 36 or 72 consecutive dates of service, excluding weekends and holidays. For some patients, KINRYS told ZC to use the date the insurance approved TMS therapy for the patient (*i.e.*, the prior authorization date) as the first date of service to put in the false NeuroStar TMS Therapy Report. For others, KINRYS said ZC should use the date the patient first received TMS (*i.e.*, the mapping session) as the first date of service in the NeuroStar TMS Therapy Report. In addition, when KINRYS received a medical record request letter from an insurance provider (including Medicare), he told ZC to create NeuroStar TMS Therapy Report with notes for each weekday, excluding holidays, for the period of time requested in the letter.

59. ZC used screenshots from the NeuroStar TMS therapy system to identify all of

KINRYS's patients who had received any amount of TMS therapy. ZC then created NeuroStar TMS Therapy Reports according to KINRYS's instructions for these patients, continuing from where AZ left off when AZ resigned. ZC created and saved all the NeuroStar TMS Therapy Reports in the practice's Dropbox account. ZC also accessed the reports AZ had created in the Dropbox account and modified them as necessary according to KINRYS's instructions.

After ZC and AZ Resign, KINRYS Has MB Create TMS Reports

60. Investigators have interviewed SB. SB worked for KINRYS at BCCR from April 2018 to September 2018. SB stated that another BCCR employee MB, who still works at BCCR, began working for KINRYS around June 2018. SB said that MB did TMS notes for KINRYS. SB explained that ZC had done the TMS notes and then ZC showed MB how to do the TMS notes for KINRYS before ZC stopped working at BCCR. When I showed SB a sample NeuroStar TMS Therapy Patient Report, which KINRYS produced in response to the HHG-OIG subpoena, she confirmed that it looked the same as the TMS notes ZC and MB had done. SB did not create the TMS Reports, but she knew that the information was "copied and pasted," meaning she knew that ZC and MB would copy a note from one date of service in the report and paste the same note to another date of service in the report.

61. SB stated that MB would sometimes tell SB and the other women working at KINRYS's office that MB could not help with certain office duties because MB had to do the TMS notes for KINRYS. The notes were kept on the office computer, but SB was not given access to them. MB was given access to the TMS notes. SB also stated that MB emailed with KINRYS a lot at their bostonclinresearch.org email addresses about the TMS notes. SB knew this because MB told SB that KINRYS and MB emailed a lot about the notes and that KINRYS

texted her about the TMS notes as well. Additionally, SB's computer at BCCR was located next to MB's computer so SB saw that MB received emails from KINRYS about the TMS notes. SB stated that MB received emails from KINRYS that the other staff members did not receive. This stood out to SB because KINRYS usually addressed emails to his office staff to all the women who worked in reception and did TMS at BCCR.

KINRYS's Billing Insurance Carriers for Psychotherapy Treatment Not Actually Provided

Patient KM

62. Patient KM began seeing KINRYS in July or August 2016 as KM was getting ready to begin college in New Hampshire, approximately one hour away from his home in Massachusetts. Patient KM wanted to start on a course of medication to treat KM's Attention Deficit Hyperactivity Disorder ("ADHD"). Patient KM saw KINRYS at his office approximately three to four times in total during the July-August 2016 timeframe. In the first week of September 2016, Patient KM left home to begin attending college in New Hampshire. While Patient KM received at least two prescriptions from KINRYS in the mail after September 2016, Patient KM never met with KINRYS and never spoke with KINRYS by phone after August 2016.

63. Patient KM's insurance carrier in the second half of 2016 was Harvard Pilgrim HealthCare ("HPHC"). Patient KM's father was the primary subscriber for the HPHC insurance carrier that covered his child, Patient KM. Patient KM's father noticed that after Patient KM left for college in New Hampshire in September 2016, he continued to receive Explanation of Benefit forms ("EOB's") from HPHC for services KINRYS allegedly provided to Patient KM. Patient KM's father estimated that his insurance carrier, HPHC, was being billed approximately

\$600 per week for services KINRYS allegedly provided to Patient KM. Patient KM's father thought this was suspicious and contacted Patient KM at college and confirmed that Patient KM was no longer seeing KINRYS. Patient KM's father contacted HPHC to complain about the EOBs pertaining to Patient KM and to make HPHC aware of the fact that Patient KM was no longer receiving therapy from KINRYS. Patient KM's father also spoke with a representative from KINRYS's office by phone and complained about the EOBs he was receiving for Patient KM's treatment, noting that Patient KM was away attending college.

64. The investigative team has obtained documentation from HPHC concerning claims submitted to HPHC's billing group for treatment purportedly provided to Patient KM. That documentation indicates KINRYS billed for psychotherapy allegedly provided to Patient KM on the following 18 different dates between September 2016 and January 2017 when Patient KM was attending college in New Hampshire:

September 2016: 14, 20, 27

October 2016: 4, 11, 18, 25

November 2016: 1, 8, 15, 22, 29

December 2016: 6, 13, 20, 27

January 2017: 3, 10.

In addition, Patient KM's father stated that he and his family – including Patient KM – were in Brazil from December 24, 2016 through January 9, 2017. It would have been impossible for Patient KM to receive psychotherapy from KINRYS at his office on December 27, 2016 and January 3, 2017. Patient KM's father also stated that he never sent a copayment to KINRYS and that Patient KM's father never received a bill from KINRYS's office indicating he owed a

copayment.

Patient SY

65. Patient SY began seeing KINRYS for TMS therapy in the summer of 2017. According to Medicare systems data, KINRYS billed Medicare \$15,870 for 26 psychotherapy sessions (and concurrent Evaluation and Management (“E&M”) services) he supposedly provided Patient SY between June 1, 2017 and September 1, 2017, including sessions provided on July 7, 10, 14, 17, 21, and 24, 2017. Similarly, in response to an IG subpoena for medical records, KINRYS turned over psychotherapy notes for 24 sessions of psychotherapy that he supposedly provided to Patient SY between 6/1/2017 and 9/1/2017, including notes for sessions on July 7, 10, 14, 17, 21, and 24. Kinrys concluded each of these 24 psychotherapy session notes with the following statement: “Time spent face to face with patient and/or family and coordination of care: 52-67 minutes.”

66. Contrary to these representations by KINRYS, Patient SY explained that he never received psychotherapy from KINRYS. ZC, who worked at KINRYS’s office, confirmed this. Moreover, records from the United States Customs and Border Patrol shows that KINRYS flew from Boston, MA to Zurich, Switzerland on July 7, 2017 and that KINRYS did not return until July 24, 2017, making it impossible for KINRYS to have provided psychotherapy to Patient SY “face to face” on July 14, 17, and 21, 2017.

Patient MS

67. Patient MS began seeing KINRYS for TMS therapy in the Spring of 2017. Patient MS denied getting psychotherapy from KINRYS. Patient MS stated that he did not see KINRYS for anything other than TMS therapy. Patient MS said he already had a psychiatrist

when he began TMS therapy at KINRYS's office; Patient MS continued to see that psychiatrist during the period he was undergoing TMS therapy. ZC confirmed that Patient MS did not do much psychotherapy with KINRYS, but that the patient would sometimes check in with KINRYS after a TMS treatment.

68. Patient MS reported, however, that Patient MS did see a "Dr. Ana" at KINRYS's office for psychotherapy. Ana O was interviewed as part of this investigation. Ana O worked as a therapist at KINRYS's Natick office from late 2016 until October 2017. Ana O reported that she is not a licensed psychologist in the U.S. but she is licensed in Brazil. Ana O stated that she saw roughly 30 of KINRYS's patients for psychotherapy visits during this time. Ana O confirmed that Patient MS was one of these patients and that she saw Patient MS for therapy sessions twice per month. Ana O stated that she is not a U.S. citizen but was supposed to be doing research under KINRYS at Massachusetts General Hospital through a J-1 Visa. She confirmed that KINRYS was aware of this.

69. Medicare systems data shows that KINRYS billed Medicare for 99 psychotherapy sessions that KINRYS supposedly provided to Patient MS between March 2017 and March 2018. This is inconsistent with the information Patient MS, Ana O and ZC provided regarding psychotherapy services allegedly provided to Patient MS at KINRYS's office. The data indicates that KINRYS usually billed Medicare for providing psychotherapy two times per week to Patient MS. According to Medicare systems data, KINRYS billed Medicare for \$60,400 for psychotherapy and the medical evaluation and management services he supposedly provided to Patient MS with the psychotherapy. The data shows Medicare reimbursed KINRYS \$14,104.48 for these services.

70. In response to an IG subpoena for medical records, KINRYS turned over psychotherapy notes for 24 sessions of psychotherapy he supposedly provided to Patient MS between June 6, 2017 and September 7, 2017. The dates of service for these notes indicate KINRYS was providing psychotherapy to Patient MS twice per week for the majority of this period of time. In the “LEVEL OF CARE JUSTIFICATION” section of each of these 24 notes, KINRYS included the following note: “Return 2x per week. Call prn.” He also included in each of the 24 notes the following statement: “Time spent face to face with patient and/or family and coordination of care: 52-67 minutes.” KINRYS’s signature is beneath this statement, at the end of each note.

**PROBABLE CAUSE TO BELIEVE THAT THE TARGET
ACCOUNTS CONTAIN EVIDENCE, FRUITS, AND
INSTRUMENTALITIES OF THE CRIMES IDENTIFIED ABOVE**

71. I submit that there is probable cause to believe that the TARGET ACCOUNTS, as well as data associated with those accounts, contain evidence, fruits, and instrumentalities of the crimes identified above.

72. The investigation to date demonstrates that KINRYS and certain BCCR office staff used the TARGET ACCOUNTS to facilitate and further the operation of KINRYS’s practice and BCCR. In particular, KINRYS emailed with BCCR staff about how to respond to letters from Medicare and other insurance carriers about claims submitted for TMS therapy treatments and psychotherapy sessions. Also, KINRYS and BCCR staff used Google calendars to schedule psychotherapy and TMS therapy appointments for their patients.

TARGET ACCOUNTS

ZC’s and KINRYS’s BCCR Email Accounts

73. According to ZC, there are several computers at BCCR: one computer is located at the front desk, two computers are located in the reception area, and one more computer is located in KINRYS's office, which only KINRYS uses.

74. ZC stated that KINRYS set up @bostonclinresearch.org email accounts for each employee at his office. Based on training and experience, I was able to determine that the @bostonclinresearch.org accounts were set up using Google as a hosting provider. Moreover, Google provided subscriber information for the TARGET ACCOUNTS, which showed the name of the subscriber, the email address, and a Google Account ID number, among other things, for each account.

75. ZC reported that, even though KINRYS had an email at Massachusetts General Hospital and an email address with AOL, KINRYS generally emailed ZC from his gkinrys@bonstonclinresearch.org account.

76. KINRYS and ZC exchanged emails from their @bostonclinresearch.org addresses about a variety of issues relating to the operation of BCCR and KINRYS's billing of patients for services he purportedly provided. For example, KINRYS emailed ZC at ZC's @bostonclinresearch.org address about patient scheduling and appointments. ZC and KINRYS also exchanged emails from their @bostonclinresearch.org accounts relating to inquiries from insurance companies concerning claims submitted for KINRYS's patients. For example, KINRYS would email ZC at ZC's @bostonclinresearch.org address to alert ZC to information KINRYS had uploaded to the Dropbox account he had set up, including information relating to the medical records requests he had received from insurance carriers and Medicare.

77. KINRYS used his gkinrys@bostonclinresearch.org account to provide ZC with

instructions relating to the creation of false NeuroStar TMS Therapy Patient reports for certain BCCR patients. After AZ quit BCCR in April 2018, KINRYS asked ZC to create NeuroStar TMS Therapy Patient reports for patients whose insurance carriers were asking for medical records concerning those TMS therapy treatments.

78. ZC said that KINRYS would email ZC a letter from an insurance carrier inquiring about a patient's claims relating to TMS therapy provided during a certain period of time. ZC understood KINRYS to be asking if ZC had created the NeuroStar TMS Therapy Patient reports for the dates covered by the insurance letter / medical records request. If a NeuroStar TMS Therapy Patient report had not been created for a particular patient during the timeframe identified in the insurance medical records request letter, ZC knew that ZC had to create – or add to – a NeuroStar TMS Therapy Patient report for that patient. KINRYS told ZC that it was important that BCCR had NeuroStar TMS Therapy Patient reports for the patients and the dates requested in the insurance letters / medical requests KINRYS received.

79. ZC informed KINRYS that ZC was leaving the country for an extended period of time in June 2018 and that, when ZC returned, ZC would no longer work at BCCR. However, when ZC returned from the trip, ZC received an email from KINRYS asking if ZC would continue to work on the responses to the medical records request letters KINRYS had received from the insurance companies.

AZ's BCCR Email Account

80. AZ reported that AZ exchanged emails with KINRYS from AZ's @bostonclinresearch.org address to KINRYS's gkinrys@bostonclinresearch.org address and, sometimes, to an email address he had at Massachusetts General Hospital. KINRYS would

email patients' prescriptions and prior authorizations to AZ through their @bostonclinresearch.org accounts. In addition, as described above, AZ sent emails to KINRYS at his @bostonclinresearch.org account about the templates to be used to create the false TMS reports.

Ana O's and MB's BCCR Email Accounts

81. Ana O, who worked as a therapist at KINRYS' office from late 2016 to October 2017, stated that she provided psychotherapy to roughly 30 of KINRYS's patients, whom KINRYS assigned to her. Ana O reported that KINRYS gave her a BCCR email address, which included her first and last name @bostonclinresearch.org. She said she and KINRYS emailed each other at their bostonclinresearch.org email addresses about matters including patients' schedules and patients' insurance coverage. Ana O showed me one such email exchange, dated August 28, 2017.

82. As described above, SB stated that KINRYS and MB emailed each other at their bostonclinresearch.org email addresses about the TMS notes that MB did for KINRYS. MB's email address is mbonorino@bostonclinresearch.org. SB knew this because when SB and MB worked together, MB told SB that MB and KINRYS would email a lot at MB's bostonclinresearch.org address about the TMS notes. Additionally, SB's computer at BCCR was next to MB's computer so SB saw that MB received emails from KINRYS about the TMS notes. MB received emails from KINRYS that the other staff members did not receive, which stood out to SB because KINRYS usually addressed emails to his office staff to all the women who worked in reception and did TMS at BCCR.

Google Calendars

83. Based on my training and experience, as well as conversations with other agents, I know that small medical practices keep track of patient scheduling and appointments using computerized calendars to which practice employees have access. Based on information from employees of BCCR, BCCR kept track of patient scheduling and appointments using computerized calendars.

84. I understand Google offers a time-management application called Google Calendar. Users are required to have a Google account in order to use this application.

85. According to subscriber information Google provided for the TARGET ACCOUNTS, each TARGET ACCOUNT comes with a variety of additional Google services, including Gmail and Google Calendar.

86. Among other things, KINRYS and certain members of his BCCR staff, including at least ZC and AZ, used a Google calendar to schedule patients. KINRYS gave access to the Google calendar to staff at BCCR so they could view the calendar and add appointments to KINRYS's schedule. ZC said that ZC and AZ entered 80-90% of the appointments into the Google calendar.

87. I have seen an example of BCCR patient appointments listed in a Google Calendar. As discussed above, Patient PM's wife requested from BCCR a list of appointments Patient PM allegedly had with KINRYS. In response, on September 4, 2018, a BCCR staff member sent to Patient PM's wife a printout titled "Boston Center for Clinical Research – Calendar – Search." According to that document, the calendar was obtained from a search of a Google calendar at <https://calendar.google.com/calendar/r/search>.

88. According to ZC, ZC had a conversation with KINRYS and told KINRYS that the Google calendar BCCR was keeping was confusing and messy because, among other things, it included appointments for TMS patients in different colors. After KINRYS purchased a second NeuroStar TMS Therapy System in early 2018, ZC stated that KINRYS created a separate Google calendar for the second NeuroStar TMS Therapy System. Google produced subscriber information for the email address tms2@bostonclinresearch.org. According to Google's response, the name of the subscriber for that email account is "TMS2 Calendar" and among the services that account has is Google Calendar. Google produced similar information for the email address tms1@bostonclinresearch.org. According to Google's response, the name of the subscriber for that email account is "TMS1 Calendar" and among the services that account has is Google Calendar.

89. As described above in connection with Patient PM, there has been at least one instance where appointments listed in the Google calendar do not match the dates listed in the NeuroStar TMS Therapy Reports that ZC and AZ created at KINRYS's direction (which KINRYS produced in response to an HHS-OIG subpoena). Also, there are appointments for Patient PM listed in the Google calendar that do not match the dates of service listed in the Medicare systems data for Patient PM. Specifically, the Google calendar sent to Patient PM's wife shows that Patient PM had 23 therapy appointments scheduled at BCCR between September 7, 2016 and January 4, 2018. According to Medicare systems data, KINRYS billed Medicare for 42 psychotherapy sessions during that same period. I submit that there is probable cause to believe that the Google calendars associated with the TARGET ACCOUNTS will show inconsistencies between the treatments KINRYS and BCCR actually provided and the treatments

for which KINRYS and BCCR billed.

90. Ana O stated that KINRYS never gave her access to his Google calendar, but that she also had a Google calendar associated with her @bostonclinresearch.org email address. Ana O said she scheduled her psychotherapy visits with patients on this calendar. Ana O also stated that KINRYS would schedule her patient visits on her @bostonclinresearch.org calendar and that KINRYS, ZC, and AZ had access to her Google calendar. AO stated that she did not keep any records of her visits with patients and did not document progress notes regarding her visits with patients. She stated that the Google calendar associated with her bostonclinresearch.org email is the only record of her visits with patients, and that it should show which patients she saw and how frequently she saw them. She would add a note to the calendar if the patient did not show up or the visit had to be rescheduled. Ana O said that she never saw patients twice per week.

91. On October 10, 2018, November 8, 2018, November 21, 2018, December 12, 2018, the U.S. Attorney's Office for the District of Massachusetts submitted to Google letters requesting that the company preserve records, under 18 U.S.C. § 2703(f), associated with the TARGET ACCOUNTS, among others, for 90 days. On January 9, 2019, the U.S. Attorney's Office for the District of Massachusetts submitted to Google a letter requesting that Google preserve records under 18 U.S.C. § 2703(f)(1) for the TARGET ACCOUNTS for an additional 90 days.

ZC's Access of Her @bostonclinresearch.org account After Leaving BCCR in October 2018

92. I interviewed ZC on the following dates between September 2018 and January 2019: September 9, 2018, October 4, 2018, October 5, 2018, October 9, 2018, October 12, 2018 and January 25, 2019. During several of these interviews, ZC had her personal laptop computer

open on a table in front of her. During several of these interviews, ZC (a) showed investigators several screenshots of her computer showing emails she exchanged with KINRYS in the past, (b) provided several emails between her and KINRYS from the time when she worked at BCCR, and (c) read aloud portions of several emails she and KINRYS had exchanged during the time ZC worked at BCCR. I assumed that, despite not working at BCCR any longer, ZC was in possession of old emails between ZC and KINRYS. At the outset of my October 12, 2018 interview with ZC, out of an abundance of caution, I told ZC that I was not asking her to access her BCCR email account (@bostonclinresearch.org) and that she should not access her BCCR email account. One reason I provided ZC with this direction was that BCCR has been represented by counsel since at least June 2018 in connection with HHS-OIG's investigation into KINRYS and BCCR's billing practices. It was during this October 12, 2018 interview that ZC made me aware, for the first time, that she still had access to her @bostonclinresearch.org email account despite the fact that she no longer worked at BCCR. I made clear at this time that ZC should not access the BCCR email system even if she was able to access to it. I never directed or asked ZC to access the BCCR email system either before or after this point in time.

93. The government is not relying on any of the emails ZC read, showed, or forwarded to investigators during the interviews with her on September 9, 2018, October 4, 2018, October 5, 2018 or October 12, 2018 to establish probable cause necessary to search and seize the TARGET ACCOUNTS.

TECHNICAL BACKGROUND

94. In my training and experience, enterprises today increasingly use cloud service providers to manage email for employees (or students, contractors, and any other individuals

associated with the enterprise), as well as for other types of information. Under this arrangement, the enterprise pays the cloud service provider to host its email accounts and data. Although the enterprise's email addresses still bear the enterprise's domain name (that is, for example, they end in "@company.com"), the service provider stores its content and helps manage access and security for the domain.

95. As described above, through this investigation, I learned that the @bostonclinresearch.org email accounts are hosted by Google.

96. In my training and experience, I have learned that email hosting companies, such as Google, maintain computer servers connected to the Internet. Through those computer servers, customers send and receive email on the Internet. Customers typically access their accounts on Google's computer servers from any computer connected to the Internet. Based on my training and experience, I know that Google is able to identify multiple Google accounts accessed from the same device by using "authentication cookies" or "machine cookies."

97. When an email user sends an email, it is initiated at the user's computer, transferred via the Internet to the computer servers of the user's email provider, and then transmitted to its end destination. Conversely, an email sent to an email recipient is transmitted to the computer servers of the recipient's email provider where it can be accessed by the recipient and transferred to the recipient's computer to be read.

98. In my training and experience, I have learned that email service providers typically allow customers to store incoming and outgoing emails on the email service provider's computer servers. These emails can be stored on the email service provider's computer servers until the customer elects to remove or delete the emails from the service provider's computer

servers, until the customer's mailbox reaches storage limitations set by the email service provider, or until other terms set by the email service provider are met. In the case of emails that are removed or deleted from the email service provider's computer servers by a customer, email service providers may retain those emails for a period of time, known as a deleted item retention period.

99. The TARGET ACCOUNTS have a variety of services and tools associated with them. Google provides dozens of these services to Google-hosted email users for personal and/or business convenience.

100. I know through my training and experience, as well as through discussions with other agents, that a Google customer can keep unread, sent and draft emails in their account indefinitely, as long as they are not deleted by the user. In addition, Google has storage capacity that allows customers to store opened incoming mail and sent mail indefinitely if they choose, subject to a maximum size limit.

101. Some email providers, including Google, also store and can provide additional information associated with and accessed through a subscriber's account including the following: address books, buddy lists, photos, files, data, Calendar, Contacts, Docs and Drive. Of importance to this investigation, and the subject of this warrant request, are the full contents of the email accounts and the Google Calendar service, as delineated in the Attachment B associated with each of the TARGET ACCOUNTS.

102. E-mail providers also typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information. Google stores and can provide this type of information.

LEGAL AUTHORITY

103. The government may obtain both electronic communications and subscriber information from an e-mail provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

104. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

105. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

106. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. Pursuant to 18 U.S.C. § 2713, the government intends to require the disclosure pursuant to the requested warrants of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBERS

107. I request that the application associated with each of the TARGET ACCOUNTS,

the warrant associated with each of the TARGET ACCOUNTS, the order associated with each of the TARGET ACCOUNTS, and any related papers be sealed by the Court until such time as the Court pursuant to Local Rule 7.2 directs otherwise.

108. I further request that, pursuant to the preclusion-of-notice provisions of 18 U.S.C. § 2705(b), the Court order Google not to notify any person (including the subscriber to whom the materials relate) of the existence of the application associated with each of the TARGET ACCOUNTS or the Court's Order associated with each of the TARGET ACCOUNTS for the earlier of one year from the date of the Court's Order or upon notice by the government within 30 days of the conclusion of its investigation, unless the Court extends such period under 18 U.S.C. § 2705(b). Non-disclosure is appropriate in this case because the Court's Order associated with each of the TARGET ACCOUNTS relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the existence of investigation. There is accordingly reason to believe that notification of the existence of the Order associated with each of the TARGET ACCOUNTS will seriously jeopardize the investigation, including by giving targets an opportunity to flee prosecution, destroy or tamper with evidence, change patterns of behavior, or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b). Moreover, some of the evidence in this investigation is stored electronically. If alerted to the existence of the Order associated with each of the TARGET ACCOUNTS, the targets could destroy that evidence, including information saved to their personal computing devices, on other electronic media, or in social media accounts.

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

109. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Google, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

110. Based on my training and experience and that of other law enforcement, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

111. The United States does not ask for this extra data or participate in its production.

112. Should Google produce late-created data in response to the warrant associated with each of the TARGET ACCOUNTS, I request permission to view all late-created data that was created by Google, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

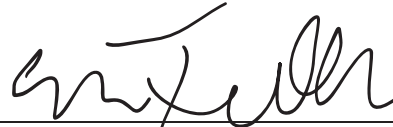
113. For these reasons, I request that the Court approve the procedures in the Attachment B associated with each of the TARGET ACCOUNTS, which set forth these limitations.

CONCLUSION

114. Based on the information described above, I have probable cause to believe that records and data from the TARGET ACCOUNTS (as described in the Attachment A associated with each of the TARGET ACCOUNTS), contain evidence, fruits, and instrumentalities of the above-listed crimes (as described in the Attachment B associated with each of the TARGET ACCOUNTS).

115. The procedures for copying and reviewing the relevant records are set out in Attachment B to the search warrant associated with each of the TARGET ACCOUNTS.

Respectfully submitted,



ERIN FULLER
Special Agent
United States Department of Health and
Human Services, Office of Inspector
General

Subscribed and sworn to before me
on Feb 13, 2019
Date



DAVID H. HENNESSY
Chief United States Magistrate Judge



ATTACHMENT A

anaornelas@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as anaornelas@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

anaornelas@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the anaornelas@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of

the United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to anaornelas@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the anaornelas@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the anaornelas@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the anaornelas@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the anaornelas@bostonclinresearch.org.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);

- c. Records of session times and durations;
 - d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the anaornelas@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C. § 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:
1. communications between or among KINRYS and BCCR staff;
 2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
 3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
 4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
 5. the scheduling of patients of BCCR or KINRYS;
 6. the work schedule of KINRYS and staff of BCCR;
 7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
 8. the identity of the persons who have owned or operated the anaornelas@bostonclinresearch.org account or any associated e-mail accounts;
 9. the existence and identity of any co-conspirators;
 10. the travel or whereabouts of the person or persons who have owned or operated the anaornelas@bostonclinresearch.org account or any associated e-mail accounts;

11. the identity, location, and ownership of any computers used to access these e-mail accounts;
12. other e-mail or Internet accounts providing Internet access or remote data storage;
13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
14. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

azawadzka@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as azawadzka@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

azawadzka@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the azawadzka@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of

the United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to azawadzka@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the azawadzka@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the azawadzka@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the azawadzka@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the azawadzka@bostonclinresearch.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);

- c. Records of session times and durations;
 - d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the azawadzka@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C. § 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:
1. communications between or among KINRYS and BCCR staff;
 2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
 3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
 4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
 5. the scheduling of patients of BCCR or KINRYS;
 6. the work schedule of KINRYS and staff of BCCR;
 7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
 8. the identity of the persons who have owned or operated the azawadzka@bostonclinresearch.org account or any associated e-mail accounts;
 9. the existence and identity of any co-conspirators;
 10. the travel or whereabouts of the person or persons who have owned or operated the azawadzka@bostonclinresearch.org account or any associated e-mail accounts;

11. the identity, location, and ownership of any computers used to access these e-mail accounts;
12. other e-mail or Internet accounts providing Internet access or remote data storage;
13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
14. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

gkinrys@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as gkinrys@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

gkinrys@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the gkinrys@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of the

United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to gkinrys@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the gkinrys@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the gkinrys@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the gkinrys@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the gkinrys@bostonclinresearch.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);
 - c. Records of session times and durations;

- d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the gkinrys@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C.

§ 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:

1. communications between or among KINRYS and BCCR staff;
2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
5. the scheduling of patients of BCCR or KINRYS;
6. the work schedule of KINRYS and staff of BCCR;
7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
8. the identity of the persons who have owned or operated the gkinrys@bostonclinresearch.org account or any associated e-mail accounts;
9. the existence and identity of any co-conspirators;
10. the travel or whereabouts of the person or persons who have owned or operated the gkinrys@bostonclinresearch.org account or any associated e-mail accounts;
11. the identity, location, and ownership of any computers used to access

these e-mail accounts;

12. other e-mail or Internet accounts providing Internet access or remote data storage;
13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
14. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

mbonorino@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as mbonorino@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

mbonorino@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the mbonorino@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of

the United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to mbonorino@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the mbonorino@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the mbonorino@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the mbonorino@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the mbonorino@bostonclinresearch.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);

- c. Records of session times and durations;
 - d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the mbonorino@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C. § 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:
1. communications between or among KINRYS and BCCR staff;
 2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
 3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
 4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
 5. the scheduling of patients of BCCR or KINRYS;
 6. the work schedule of KINRYS and staff of BCCR;
 7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
 8. the identity of the persons who have owned or operated the mbonorino@bostonclinresearch.org account or any associated e-mail accounts;
 9. the existence and identity of any co-conspirators;
 10. the travel or whereabouts of the person or persons who have owned or operated the mbonorino@bostonclinresearch.org account or any associated e-mail accounts;

11. the identity, location, and ownership of any computers used to access these e-mail accounts;
12. other e-mail or Internet accounts providing Internet access or remote data storage;
13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
14. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

tms1@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as tms1@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

tms1@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the tms1@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of the

United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to tms1@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the tms1@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the tms1@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the tms1@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the tms1@bostonclinresearch.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);
 - c. Records of session times and durations;

- d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the tms1@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C.

§ 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:

1. communications between or among KINRYS and BCCR staff;
2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
5. the scheduling of patients of BCCR or KINRYS;
6. the work schedule of KINRYS and staff of BCCR;
7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
8. the identity of the persons who have owned or operated the tms1@bostonclinresearch.org account or any associated e-mail accounts;
9. the existence and identity of any co-conspirators;
10. the travel or whereabouts of the person or persons who have owned or operated the tms1@bostonclinresearch.org account or any associated e-mail accounts;
11. the identity, location, and ownership of any computers used to access these e-mail accounts;

12. other e-mail or Internet accounts providing Internet access or remote data storage;
 13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
 14. The existence or location of paper print-outs of any data from any of the above.
- B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

tms2@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as tms2@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

tms2@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the tms2@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of the

United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to tms2@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the tms2@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the tms2@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the tms2@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the tms2@bostonclinresearch.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);
 - c. Records of session times and durations;

- d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the tms2@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C.

§ 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:

1. communications between or among KINRYS and BCCR staff;
2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
5. the scheduling of patients of BCCR or KINRYS;
6. the work schedule of KINRYS and staff of BCCR;
7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
8. the identity of the persons who have owned or operated the tms2@bostonclinresearch.org account or any associated e-mail accounts;
9. the existence and identity of any co-conspirators;
10. the travel or whereabouts of the person or persons who have owned or operated the tms2@bostonclinresearch.org account or any associated e-mail accounts;
11. the identity, location, and ownership of any computers used to access these e-mail accounts;

12. other e-mail or Internet accounts providing Internet access or remote data storage;
13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
14. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT A

zcarvalho@bostonclinresearch.org

The premises to be searched and seized are (1) the e-mail account identified as zcarvalho@bostonclinresearch.org, (2) other user-generated data stored with that account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and via the website <https://support.google.com/legal-investigations/contact/LERS>.

ATTACHMENT B

zcarvalho@bostonclinresearch.org

I. Search Procedure

- A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the account and files to be searched, as described in Section II below.
- B. Google will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).
- C. Google will provide the account duplicate to law enforcement personnel.
- D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.
- E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Google after fourteen days from the warrant's issue (“late-created data”), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Google without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Google Personnel

- A. All data files associated with the zcarvalho@bostonclinresearch.org account within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of

the United States,” *see* 18 U.S.C. § 2713, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
2. The contents of all text or instant messages;
3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
4. The contents of all calendar data;
5. Lists of friends, buddies, contacts, or other subscribers;
6. Records of any Google accounts that are linked to zcarvalho@bostonclinresearch.org by machine cookies or authentication cookies (i.e., all Google usernames that logged into Google from the same device that was used to access the zcarvalho@bostonclinresearch.org);
7. Records pertaining to communications between Google and any person regarding the zcarvalho@bostonclinresearch.org account and any e-mail accounts associated with that address, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the zcarvalho@bostonclinresearch.org account and any associated e-mail accounts, including:

1. Subscriber information for the zcarvalho@bostonclinresearch.org account and any associated e-mail accounts:
 - a. Name(s) and account identifiers;
 - b. Address(es);
 - c. Records of session times and durations;

- d. Length of service (including start date) and types of service utilized;
 - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
 - f. The means and source of payment for such service (including any credit card or bank account number); and
 - g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for any connections to or from the zcarvalho@bostonclinresearch.org account and any associated e-mail accounts, including:
- a. Connection time and date;
 - b. Disconnect time and date;
 - c. The IP address that was used when the user connected to the service;
 - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
 - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

- A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1347, 18 U.S.C.

§ 1343; 18 U.S.C. § 1035, and 42 U.S.C. § 1320a-7b(b), including records from January 1, 2015 through the present relating to:

1. communications between or among KINRYS and BCCR staff;
2. communications between KINRYS and BCCR staff, on the one hand, and patients of KINRYS and BCCR staff, on the other hand;
3. communications between KINRYS and BCCR staff, on the one hand, and insurance carriers, including Medicare, or billing companies, on the other hand;
4. the treatment of patients of BCCR or KINRYS, including medical records for those patients;
5. the scheduling of patients of BCCR or KINRYS;
6. the work schedule of KINRYS and staff of BCCR;
7. payment or reimbursement for treatment provided or purportedly provided to patients of BCCR or KINRYS;
8. the identity of the persons who have owned or operated the zcarvalho@bostonclinresearch.org account or any associated e-mail accounts;
9. the existence and identity of any co-conspirators;
10. the travel or whereabouts of the person or persons who have owned or operated the zcarvalho@bostonclinresearch.org account or any associated e-mail accounts;
11. the identity, location, and ownership of any computers used to access

these e-mail accounts;

12. other e-mail or Internet accounts providing Internet access or remote data storage;
13. the existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
14. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature